

UNIVERSITY OF TECHNOLOGY, SYDNEY  
Faculty of Engineering and Information Technology

# **INNOVATIVE MACHINE LEARNING TECHNIQUES FOR SECURITY DETECTION PROBLEMS**

A dissertation submitted for the degree of  
Doctor of Philosophy in Computing Sciences

By

**Tich Phuoc Tran**

Sydney, Australia

2009

# CERTIFICATE OF ORIGINALITY

UNIVERSITY OF TECHNOLOGY, SYDNEY

Faculty of Engineering and Information Technology

C02029 Doctor of Philosophy in Computing Sciences

CERTIFICATE OF ORIGINALITY

Of Project Work

I certify that the work in this thesis has not previously been submitted for a degree nor has it been submitted as part of requirements for a degree except as fully acknowledged within the text.

I also certify that the thesis has been written by me. Any help that I have received in my research work and the preparation of the thesis itself has been acknowledged. In addition, I certify that all information sources and literature used are indicated in the thesis.

Signature of candidate



A handwritten signature in dark ink, written over a horizontal dashed line. The signature is stylized and appears to be a cursive representation of a name.

## ACKNOWLEDGEMENTS

Undertaking and completing a task like this would not have been possible without the encouragement and support of many individuals.

First and foremost, I would like to pay my respects and thanks to my principle supervisors, Dr. Tony Jan and Dr. Xiangjian He, for their technical ideas and constructive criticism which has significantly contributed to the success of this thesis. Their professional advice has been a great asset to have during my moments of confusion and I truly acknowledge that.

I extend my thanks to Prof. Tom Hintz, who critiqued the drafts and offered valuable suggestions concerning the content and layout of the report.

I wish to thank Dr. Andy Simmonds for being a constant source of guidance throughout the course of this thesis, especially in understanding the different aspects of networks, which was truly needed at the beginning.

I also acknowledge great help and cooperation that I received from my colleagues, Dr. Qiang Wu, Dr. Longbing Cao and Mr. Pohsiang Tsai.

I am grateful to my brother, Mr. Timmy Tran, for his sense of humor and support during my PhD candidature.

Last but not least, I would also like to thank my parents, who gave me the opportunity for my education and supported me in every direction. Their love and care enabled me to ease my mind and soul so that I could concentrate on this thesis.

Sydney, Australia, April, 2009.

## ABSTRACT

Most of the currently available network security techniques cannot cope with the dynamic and increasingly complex nature of the attacks on distributed computer systems. Therefore, an automated and adaptive defensive tool is imperative for computer networks. Alongside the existing techniques for preventing intrusions such as encryption and firewalls, Intrusion Detection System (IDS) technology has established itself as an emerging field that is able to detect unauthorized access and abuse of computer systems from both internal users and external offenders. Most of the novel approaches in this field have adopted Artificial Intelligence (AI) technologies such as Artificial Neural Networks (ANN) to improve detection performance. The true power and advantage of ANN lie in its ability to represent both linear and non-linear underlying functions and learn these functions directly from the data being modeled. However, ANN is computationally expensive due to its demanding processing power and this leads to the *overfitting* problem, i.e. the network is unable to extrapolate accurately once the input is outside of the training data range. These limitations challenge security systems with low detection rate, high false alarm rate and excessive computation cost. In this research, a novel Machine Learning (ML) algorithm is developed to alleviate those difficulties of conventional detection techniques used in available IDS. By implementing *Adaptive Boosting* and *Semi-parametric radial-basis-function neural networks*, this model aims at minimizing learning bias (how well the model fits the available sample data) and generalization variance (how stable the model is for unseen instances) at an affordable cost of computation. The proposed method is applied to a set of *Security Detection Problems* which aim to detect security breaches within computer networks. In particular, we consider two benchmarking problems: intrusion detection and anti-spam filtering. It is empirically shown that our technique outperforms other state-of-the-art predictive algorithms in both of the problems, with significantly increased detection accuracy, minimal false alarms and relatively low computation.



# PUBLICATIONS

## ■ Book chapters

- **T.P. Tran**, P. Tsai, T. Jan, X. He, 2008, "Machine Learning Techniques for Network Security Detection Problems", *Dynamic and Advanced Data Mining for Progressing Technological Development: Innovations and Systemic Approaches* (Ed. ABM.S. Ali and Y. Xiang), IGI Publishing, Pennsylvania, USA
- **T.P. Tran**, P. Tsai, X. He, T. Jan, 2009, "Network Intrusion Detection using Multi-expert Classification and Voting Techniques", *Machine Learning*, ISBN 978-953-7619-X-X, I-Tech Education and Publishing, Vienna, Austria (accepted)
- **T.P. Tran**, X. He, T. Jan, 2009, "Spam Recognition using Linear Regression combined with a Radial Basis Function Network ", *Pattern Recognition*, ISBN 978-953-7619-X-X, I-Tech Education and Publishing, Vienna, Austria (submitted)
- P. Tsai, **T.P. Tran** , T. Hintz, T. Jan, 2008, "Discriminant Subspace Analysis for Uncertain Situation in Facial Recognition", *Face Recognition*, (Ed. Kresimir Delac, Mislav Grgic, Marian Stewart Bartlett), I-Tech Education and Publishing, Vienna, Austria

## ■ Conference Papers

- **T.P. Tran**, P. Tsai, T. Jan, 2008, "A Multi-Expert Classification Framework with Transferable Voting for Intrusion Detection", *The Seventh International Conference on Machine Learning and Applications (ICMLA'08)*, California, USA. (tier-A conference)
- **T.P. Tran**, P. Tsai, T. Jan, 2008, "An Adjustable Combination of Linear Regression and Modified Probabilistic Neural Network for Anti-Spam

Filtering”, *The 19th International Conference on Pattern Recognition (ICPR)*, Florida, USA. (**tier-A conference**)

- ❑ **T.P. Tran**, D. Wang, S. Chen, M. Tolentino, J. Lu, 2006, “A neural network classifier based decision support system (NNCDSS) for network intrusion detection and response”, *International Conference on Intelligent Systems and Knowledge Engineering (ISKE2006)*, Shanghai, China (in press)
- ❑ **T.P. Tran**, T. Jan, 2006, “Boosted Modified Probabilistic Neural Network (BMPNN) for Network Intrusion Detection”, *Proc. of IEEE International Joint Conference in Neural Networks (IEEE-IJCNN)*, Vancouver, BC, Canada. (**tier-A conference**)
- ❑ **T.P. Tran**, T. Jan, A.J. Simmonds, 2006, “A Multi-Expert Classification Framework for Network Misuse Detection”, *Proc. of IASTED International Conference in Artificial Intelligence and Soft Computing (AISC 2006)*, Palma de Mallorca, Spain. (**tier-A conference**)
- ❑ P. Tsai, **T.P. Tran**, T. Hintz, T. Jan, 2008, "An Evaluation of Bi-modal Facial Appearance+Facial Expression Face Biometrics", *The 19th International Conference on Pattern Recognition (ICPR)*, Florida, USA. (**tier-A conference**)
- ❑ P. Tsai, **T.P. Tran**, T. Hintz, T. Jan, 2008, "Adaptive Multiple Experts System for Personal Identification Using Facial Behaviour Biometrics", *IEEE International Workshop on Multimedia Signal Processing (MMSP)*, Cairns, Queensland, Australia. (**tier-A conference**)
- ❑ T. Jan, **T.P. Tran**, 2005, “Effective Coding using Locality-Enhanced Support Vector Machines: Theoretical Perspectives”, *Proc. of IEEE International Joint Conference in Neural Networks (IEEE-IJCNN)*, Montreal, Canada. (**tier-A conference**)

- Y.Y Chung, P. Wang, X. Chen, C. Bae, A.F. Otoom, **T.P., Tran**, 2005,  
“A Performance Comparison of High Capacity Digital Watermarking  
Systems”, *Proc. of International Conference on Knowledge-Based &  
Intelligent Information & Engineering Systems (KES)*, 14-16, Melbourne,  
Australia

# TABLE OF CONTENTS

**ACKNOWLEDGEMENTS..... III**

**ABSTRACT .....IV**

**PUBLICATIONS..... V**

**TABLE OF CONTENTS..... 1**

**LIST OF FIGURES ..... 7**

**LIST OF TABLES ..... 9**

**ABBREVIATIONS ..... 10**

**CHAPTER 1. INTRODUCTION ..... 12**

1.1. Overview.....12

1.2. Research Significance and Contributions .....14

1.3. Research Motivations.....16

1.4. Research Objectives .....18

1.5. Organization of the Thesis .....19

**CHAPTER 2. NETWORK SECURITY AND CLASSIFICATION PROBLEMS ..... 22**

2.1. Rationale of Network Security.....22

2.2. Some Widely Publicized Attacks .....23

2.3. Definition of Intrusion Detection System .....24

2.4. History of Intrusion Detection Technology .....25

2.5. Spamming and Its Impacts .....26

2.5.1. Overview of spamming .....26

2.5.2. Impacts of spamming and preventive techniques .....28



|   |   |           |
|---|---|-----------|
| 2.6.  | Security Detection Problems.....                      | 29        |
| 2.7.  | Chapter Summary.....                                  | 30        |
| <b>CHAPTER 3. CLASSIFICATION OF INTRUSION DETECTION SYSTEMS .....</b> |   | <b>32</b> |
| 3.1.  | IDS Classification Based on Analysis Approach.....    | 32        |
| 3.1.1.  | Misuse-based Detection.....                           | 32        |
| 3.1.2.  | Anomaly-based Detection .....                         | 34        |
| 3.1.3.  | Comparison.....                                       | 35        |
| 3.2.  | IDS Classification Based on Placement of IDS .....    | 36        |
| 3.2.1.  | Host based IDS .....                                  | 36        |
| 3.2.2.  | Network based IDS .....                               | 37        |
| 3.2.3.  | Comparison.....                                       | 37        |
| 3.3.  | IDS Classification Based on Detection Timeliness..... | 38        |
| 3.3.1.  | Audit trail IDS.....                                  | 38        |
| 3.3.2.  | Real-time IDS .....                                   | 39        |
| 3.3.3.  | Comparison.....                                       | 40        |
| 3.4.  | Challenges of Current IDS.....                        | 40        |
| 3.4.1.  | Speed .....   | 40        |
| 3.4.2.  | Accuracy.....   | 41        |
| 3.4.3.  | Adaptability .....                                    | 41        |
| 3.5.  | Chapter Summary.....                                  | 42        |
| <b>CHAPTER 4. MACHINE LEARNING AND SECURITY CLASSIFICATION .....</b>  |   | <b>43</b> |
| 4.1.  | Overview.....   | 43        |
| 4.1.1.  | Learning approaches .....                             | 44        |
| 4.1.2.  | Overfitting problem.....                              | 45        |
| 4.1.3.  | A data mining framework for IDS .....                 | 47        |
| 4.2.  | General Machine Learning Techniques .....             | 49        |
| 4.2.1.  | Expert Systems.....                                   | 49        |
| 4.2.2.  | Instance-Based and K-Nearest Neighbors Learning ..... | 50        |
| 4.2.3.  | Naïve Bayesian .....                                  | 52        |
| 4.2.4.  | Kernel Density Estimation.....                        | 53        |
| 4.2.5.  | Association Rules.....                                | 54        |
| 4.2.6.  | Decision Trees .....                                  | 55        |
| 4.2.7.  | Neural Networks .....                                 | 56        |
| 4.2.8.  | Genetic Algorithms .....                              | 58        |
| 4.2.9.  | Support Vector Machines .....                         | 58        |

|                   |  |           |
|-------------------|--|-----------|
| 4.2.10.           | Multiple Sensor Fusion.....  | 60        |
| 4.2.11.           | Immune System.....   | 60        |
| <b>4.3.</b>       | <b>The Intrusion Detection Contest KDD-99.....</b>                 | <b>61</b> |
| 4.3.1.            | The first-prize winning entry of the KDD-99 .....                  | 62        |
| 4.3.2.            | The second-prize winning entry of the KDD-99 .....                 | 62        |
| 4.3.3.            | The third-prize winning entry of the KDD-99 .....                  | 63        |
| 4.3.4.            | Classifying rare classes via two-phased rule induction.....        | 64        |
| <b>4.4.</b>       | <b>Real-world Examples of Intrusion Detection System .....</b>     | <b>66</b> |
| 4.4.1.            | Snort IDS .....  | 66        |
| 4.4.2.            | Pakemon IDS .....  | 66        |
| 4.4.3.            | Cisco IOS IDS.....   | 66        |
| <b>4.5.</b>       | <b>Chapter Summary.....</b>  | <b>67</b> |
| <b>CHAPTER 5.</b> | <b>NEURAL NETWORKS.....</b>  | <b>68</b> |
| <b>5.1.</b>       | <b>Artificial Neural Network.....</b>                              | <b>68</b> |
| 5.1.1.            | Multilayer Perceptron.....   | 69        |
| 5.1.2.            | Radial Basis Function Neural Network (RBFNN) .....                 | 70        |
| 5.1.3.            | Probabilistic Neural Network (PNN) .....                           | 73        |
| 5.1.4.            | Generalized Regression Neural Network (GRNN).....                  | 75        |
| 5.1.5.            | Vector Quantized GRNN (VQ-GRNN) .....                              | 78        |
| 5.1.6.            | Comparison between RBF networks.....                               | 82        |
| <b>5.2.</b>       | <b>Bias and Variance Decomposition .....</b>                       | <b>84</b> |
| <b>5.3.</b>       | <b>Parametric, non-parametric and semi-parametric models .....</b> | <b>87</b> |
| <b>5.4.</b>       | <b>Chapter Summary.....</b>  | <b>89</b> |
| <b>CHAPTER 6.</b> | <b>ENSEMBLE LEARNING .....</b>                                     | <b>90</b> |
| <b>6.1.</b>       | <b>Introduction.....</b>   | <b>90</b> |
| 6.1.1.            | Overview .....   | 90        |
| 6.1.2.            | Single-classifier versus ensemble methods .....                    | 91        |
| <b>6.2.</b>       | <b>Strategies for combining different learners .....</b>           | <b>93</b> |
| 6.2.1.            | Linear Combination.....  | 93        |
| 6.2.2.            | Non-Linear Combination.....  | 93        |
| 6.2.3.            | Mixtures of Experts.....   | 95        |
| <b>6.3.</b>       | <b>Ensemble learning techniques .....</b>                          | <b>95</b> |
| 6.3.1.            | Bagging.....   | 96        |
| 6.3.2.            | Boosting.....  | 97        |

|             |   |            |
|-------------|---|------------|
| 6.3.3.      | Comparison of Bagging and Boosting .....                | 102        |
| <b>6.4.</b> | <b>Model Diversity .....</b>                            | <b>102</b> |
| 6.4.1.      | Overview .....  | 102        |
| 6.4.2.      | Measure of Diversity .....                              | 104        |
| <b>6.5.</b> | <b>Margin Theory .....</b>                              | <b>107</b> |
| 6.5.1.      | Overview .....  | 107        |
| 6.5.2.      | Error bounds of Boosting .....                          | 109        |
| <b>6.6.</b> | <b>Critiques of Diversity and Margin Theories .....</b> | <b>113</b> |
| <b>6.7.</b> | <b>Chapter summary .....</b>                            | <b>115</b> |

## **CHAPTER 7. BOOSTED MODIFIED PROBABILISTIC NEURAL NETWORK . 117**

|             |  |            |
|-------------|--|------------|
| <b>7.1.</b> | <b>Problem statements.....</b>                         | <b>117</b> |
| 7.1.1.      | Proposal Motivations.....                              | 117        |
| 7.1.2.      | Proposal Objectives.....                               | 119        |
| <b>7.2.</b> | <b>BMPNN's theory .....</b>                            | <b>120</b> |
| 7.2.1.      | Overall System.....                                    | 121        |
| 7.2.2.      | Adaptive Booster (master algorithm).....               | 122        |
| 7.2.3.      | Modified Probabilistic Classifier (Base Learner) ..... | 124        |
| <b>7.3.</b> | <b>Remarks on BMPNN's features .....</b>               | <b>127</b> |
| <b>7.4.</b> | <b>Chapter Summary.....</b>                            | <b>128</b> |

## **CHAPTER 8. RESEARCH DESIGN AND METHODOLOGY ..... 130**

|             |   |            |
|-------------|---|------------|
| <b>8.1.</b> | <b>Pattern classification problem .....</b>             | <b>130</b> |
| <b>8.2.</b> | <b>Measure Classification Performance.....</b>          | <b>131</b> |
| 8.2.1.      | Common Measures of Performance.....                     | 131        |
| 8.2.2.      | Problems with simple performance measures .....         | 134        |
| 8.2.3.      | ROC Analysis .....                                      | 134        |
| 8.2.4.      | Estimating the predictive accuracy of a classifier..... | 136        |
| <b>8.3.</b> | <b>Tools and platforms .....</b>                        | <b>137</b> |
| 8.3.1.      | Common tools and platforms.....                         | 137        |
| 8.3.2.      | An implementation for BMPNN.....                        | 137        |
| <b>8.4.</b> | <b>Chapter Summary.....</b>                             | <b>139</b> |

## **CHAPTER 9. APPLICATION TO NETWORK INTRUSION DETECTION..... 141**



|   |                |
|---|----------------|
| <b>9.1. Overview.....</b>   | <b>141</b>     |
| 9.1.1. Related works.....   | 141            |
| 9.1.2. Intrusion detection data .....                                     | 143            |
| 9.1.3. Evaluation Techniques .....  | 148            |
| <b>9.2. Experiments on the KDD-99 data.....</b>                           | <b>151</b>     |
| 9.2.1. Experiment design.....   | 151            |
| 9.2.2. Experiment results.....  | 154            |
| <b>9.3. Handling rare and difficult attacks .....</b>                     | <b>155</b>     |
| 9.3.1. Multi-Expert Classification Framework (MECF).....                  | 155            |
| 9.3.2. Voting techniques for pattern recognition .....                    | 157            |
| 9.3.3. Experimental analysis.....   | 159            |
| <b>9.4. Chapter Summary.....</b>  | <b>167</b>     |
| <br><b>CHAPTER 10. APPLICATION TO ANTI-SPAM FILTERING.....</b>            | <br><b>169</b> |
| <b>10.1. Introduction.....</b>  | <b>169</b>     |
| 10.1.1. Spam recognition as a challenging task.....                       | 170            |
| 10.1.2. Machine learning for spam recognition.....                        | 171            |
| 10.1.3. Ling-Spam benchmark .....   | 172            |
| <b>10.2. Spam recognition methods.....</b>                                | <b>173</b>     |
| 10.2.1. Naïve Bayes .....   | 173            |
| 10.2.2. Memory based learning .....                                       | 173            |
| 10.2.3. Boosted Decision Tree.....  | 174            |
| 10.2.4. Support Vector Machine.....                                       | 175            |
| 10.2.5. Artificial Neural Network.....                                    | 175            |
| <b>10.3. Classification framework for spam recognition.....</b>           | <b>175</b>     |
| 10.3.1. Description.....  | 176            |
| 10.3.2. Performance evaluation .....                                      | 179            |
| <b>10.4. Experiments and results.....</b>                                 | <b>183</b>     |
| 10.4.1. Experiment design.....  | 183            |
| 10.4.2. Experiment results.....   | 184            |
| <b>10.5. Chapter summary .....</b>  | <b>188</b>     |
| <br><b>CHAPTER 11. CONCLUSIONS AND FUTURE RESEARCH.....</b>               | <br><b>190</b> |
| <b>11.1. Summary and Conclusions .....</b>                                | <b>190</b>     |
| <b>11.2. Future Research .....</b>  | <b>192</b>     |
| 11.2.1. Distributed Intrusion Detection: multi-level agent technique..... | 192            |

|  |            |
|--|------------|
| 11.2.2. Incorporating prior domain knowledge into Machine Learning ..... | 193        |
| <b>APPENDICES.....</b>   | <b>197</b> |
| <b>Appendix A: Terminologies.....</b>                                    | <b>197</b> |
| <b>Appendix B: Notes on relevant topics .....</b>                        | <b>200</b> |
| B.1 Vapnik-Chervonenkis dimension .....                                  | 200        |
| B.2 Lagrangian Multiplier .....  | 200        |
| B.3 Boosting from the view of Game Theory .....                          | 202        |
| B.4 Multiclass boosting using error correcting.....                      | 204        |
| <b>Appendix C: The KDD-99 Dataset.....</b>                               | <b>205</b> |
| <b>Appendix D: Data preprocessing.....</b>                               | <b>208</b> |
| <b>Appendix E: MATLAB code for BMPNN .....</b>                           | <b>212</b> |
| <b>REFERENCES.....</b>   | <b>230</b> |



# LIST OF FIGURES

|  |     |
|--|-----|
| Figure 3-1: Misuse Detection Method .....  | 33  |
| Figure 3-2: Anomaly Detection Method .....                                       | 35  |
| Figure 3-3: Audit Trail Processing Method.....                                   | 38  |
| Figure 3-4: Real time Intrusion Detection Method .....                           | 39  |
| Figure 4-1: Multiple functions fit the same data.....                            | 46  |
| Figure 4-2: Overfitting problem.....   | 47  |
| Figure 4-5: Decision Tree.....   | 56  |
| Figure 4-9: A neuron in Neural Network .....                                     | 57  |
| Figure 4-10: Optimal separating hyperplane in SVM .....                          | 59  |
| Figure 4-11: Decision for smurf attacks .....                                    | 63  |
| Figure 4-12: PN rule classification.....   | 65  |
| Figure 5-1: Architecture of Radial Basis Function Neural Network .....           | 71  |
| Figure 5-2: Surface generated by a two dimensional Gaussian function .....       | 73  |
| Figure 5-3: Architecture of Probabilistic Neural Network .....                   | 74  |
| Figure 5-4: Architecture of Generalized Regression Neural Network.....           | 77  |
| Figure 5-5: Architecture of Vector Quantized GRNN (VQ-GRNN).....                 | 80  |
| Figure 5-6: Clustering input space in Modified Probabilistic Neural Network..... | 81  |
| Figure 5-7: Risk function over model complexity .....                            | 86  |
| Figure 5-8: Parametric, non-parametric and semi-parametric learning .....        | 88  |
| Figure 6-1: Mixture of Experts Architecture .....                                | 95  |
| Figure 6-2: Update factor of AdaBoost.....                                       | 100 |
| Figure 7-1: BMPNN high-level design view .....                                   | 121 |
| Figure 8-1: Receiver Operative Characteristics (ROC) curve .....                 | 135 |
| Figure 8-2: BMPNN implementation: overall packages .....                         | 138 |
| Figure 8-3: BMPNN implementation: main class and interfaces .....                | 139 |
| Figure 9-1: Simplified version of DARPA 98 Simulation Network.....               | 143 |
| Figure 9-2: Multi-expert classifier for Intrusion Detection .....                | 156 |
| Figure 9-3: Multi-expert classification framework (MECF) .....                   | 159 |
| Figure 9-4: Detection Rate comparision.....                                      | 166 |

|  |     |
|--|-----|
| Figure 9-5: False Alarm comparision.....                                 | 167 |
| Figure 10-1: Proposed anti-spam filtering framework.....                 | 176 |
| Figure 10-2: TCR score of spam recognition methods .....                 | 185 |
| Figure 10-3: Spam precision and recall of spam recognition methods ..... | 187 |

# LIST OF TABLES

|  |     |
|--|-----|
| Table 3-1: Comparison of real time and audit-trail Intrusion Detection methods ..... | 40  |
| Table 4-1: Kernel Functions .....  | 54  |
| Table 4-2: Basic measures of Rule Interestingness.....                               | 55  |
| Table 4-3: Accuracy of the KDD-99 winner on different attack categories.....         | 62  |
| Table 6-1: Bagging Algorithm.....  | 96  |
| Table 6-2: AdaBoost Algorithm .....  | 100 |
| Table 8-1: Confusion matrix for a two-class problem .....                            | 131 |
| Table 8-2: Special cases for classification performance .....                        | 133 |
| Table 9-1: Attack types and major categories in the KDD-99 dataset.....              | 145 |
| Table 9-2 Basic, Traffic and Content Features in the KDD-99 dataset .....            | 146 |
| Table 9-3: Component sets of the KDD-99 Dataset .....                                | 147 |
| Table 9-4: Cost matrix for the KDD-99 dataset.....                                   | 150 |
| Table 9-5: Overall performance comparison between different algorithms.....          | 154 |
| Table 9-6: Detection Rate of BMPNN and KDD-99 winner.....                            | 154 |
| Table 9-7: Detection rate for different classes and features .....                   | 162 |
| Table 9-8: Local experts configuration .....   | 163 |
| Table 9-9: Detection Rate (DR %) and False Alarm Rate (FAR %) comparison .....       | 164 |
| Table 10-1: Precision/Recall evaluation on Ling-Spam data .....                      | 187 |
| Table 10-2: Computation Time, Memory size evaluation on Ling-Spam data .....         | 188 |

## ABBREVIATIONS

| Abbreviations | Descriptions  |
|---------------|---|
| AAFID         | Autonomous Agents for Intrusion Detection   |
| ACM SIGKDD    | Association for Computing Machinery Special Interest Group on Knowledge Discovery and Data Mining |
| AI            | Artificial Intelligence   |
| ANN           | Artificial Neural Network   |
| BMPNN         | Boosted Modified Probabilistic Neural Network   |
| BT            | Boosted Tree  |
| CBBF          | Common Bandwidth Basis Function   |
| DARPA         | The Defense Advanced Research Projects Agency   |
| DoS           | Denial of Service attack  |
| DR            | Detection Rate  |
| FAR           | False Alarm Rate  |
| IB            | Instance Based  |
| ICMP          | Internet Control Message Protocol   |
| IDES          | Intrusion Detection Expert System   |
| IDS           | Intrusion Detection System  |
| IPS           | Intrusion Prevent System  |
| IRC           | Internet Relay Chat   |
| i.i.d.        | Independent and identically distributed   |
| DIDS          | Distributed Intrusion Detection System  |
| GA            | Genetic Algorithm   |
| GRNN          | Generalized Regression Neural network   |
| KDD           | Knowledge Discovery & Data Mining   |
| KM            | Kernel Miner  |
| LCRF          | Layered Conditional Random Fields   |
| LR            | Logistic Regression   |
| MIT           | Massachusetts Institute of Technology   |
| ML            | Machine Learning  |
| MLP           | Multilayer Perceptron   |
| MECF          | Multi-expert classification framework   |
| MECF-MV       | Multi-expert classification framework using majority voting                                       |
| MECF-SR       | Multi-expert classification framework using Sum rule  |
| MECF-PR       | Multi-expert classification framework using Product rule  |
| MECF-STV      | Multi-expert classification framework using Single Transferable Voting                            |
| MPNN          | Modified Probabilistic Neural Network   |
| MSE           | Mean squared error  |
| NB            | Naïve Bayesian  |
| PDF           | Probability Density Function  |
| PLR           | Protocol-based Logistic Regression  |
| PNN           | Probabilistic Neural Network  |
| R2L           | Remote to local attack  |
| RAM           | Random access memory  |
| RBF           | Radial Basis Function   |

|         |  |
|---------|--|
| RBFNN   | Radial Basis Function Neural Network                                   |
| RPROP   | Resilient Propagation Neural Network                                   |
| SAMME   | Stagewise Additive Modeling using Multiclass Exponential loss function |
| SOM     | Self-Organizing Map  |
| SMO     | Sequential Minimal Optimization  |
| SVM     | Support vector machine   |
| TCP     | Transmission Control Protocol  |
| U2R     | User to root attack  |
| UBE     | Unsolicited bulk email   |
| UCE     | Unsolicited commercial email   |
| UDP     | User Datagram Protocol   |
| VQ-GRNN | Vector quantized GRNN  |